SAN DIEGO STATE UNIVERSITY
Electrical and Computer Engineering
College of Engineering

Summer 2021 Newsletter

5500 Campanile Drive
San Diego, CA 92182-1309
Phone: (619) 594-7013
Room: E-426
electrical.sdsu.edu

FACULTY AWARDS

Dr. Junfei Xie Receives the NSF CAREER Award

Dr. Junfei Xie, Assistant Professor in the Department of Electrical and Computer Engineering, received the NSF Faculty Early Career Development (CAREER) Award, which is the NSF's most prestigious award for early-career faculty. The title of the project supported by this award is "Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework". This 5-year project aims to develop an innovative theoretical framework to enable networked airborne computing, which relies on the airborne network formed by aerial vehicles with direct flight-to-flight communication links to achieve computing in the air. Click Drones that Can Calculate, Communicate, and Solve Complex Problems for the SDSU article.

Dr. Mahasweta Sarkar Receives the 2021 Diversity Excellence Award

The Diversity Excellence Award recognizes faculty, staff and alumni/community members who have shown an exemplary commitment to diversity, inclusion and social justice. Nominees were evaluated for their quality and their contribution to diversity and social justice. Dr. Mahasweta Sarkar is a Professor in the Department of Electrical and Computer Engineering. She received her doctorate degree from University of California, San Diego. She is currently the Chair of the Diversity, Equity and Inclusion committee in the College of Engineering at SDSU and serves as the College's liaison to the University's DDI Council.

SPECIAL ISSUE ON CYBERSECURITY

As we write this newsletter, the Russian cybercriminal group REvil has forced the closing of hundreds of businesses internationally that use the Kaseya VSA IT Management application. Known as the Kaseya VSA Supply-Chain Ransomware Attack, criminals are currently asking for $5M in extortion to release keys that decrypt the data of affected users. The malicious code vector was delivered over a network through an automated software update. Since the beginning of 2021, ransomware cyberattacks have targeted major businesses such as the Colonial Pipeline, Steamship Authority of Massachusetts, JBS S.A. meat processing company, and Washington DC Metropolitan Police Department. JBS paid $11 million in ransom and Colonial Pipeline paid $4.4 million in ransom to decrypt critical company data. Ransomware and other malware codes typically become installed on unsuspecting victim's computers through email messages that contain malicious attachments, web-based downloads, social media, and instant messaging applications. Through a grant from the Office of Naval Research (ONR), faculty member Dr. Christopher Paolini in the Department of Electrical and Computer Engineering is developing methods to detect and disrupt ransomware and malware cyberattacks using artificial neural network architectures embedded in hardware accelerated SmartNICs (network interface controllers) to classify and disable, at line-speed, malware transmitted on high-speed (100Gbps+) networks without imposing significant latency in packet forwarding.

Dr. Christopher Paolini

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks usually aim to access, change, or destroy sensitive information; extorting money from users (e.g. ransomware); or interrupting normal business processes (making servers inaccessible, etc.). With the advances in communication technology and the Internet of Things, currently a lot of devices (not just regular computers or mobile devices) are connected to the Internet. This phenomenon makes devices more accessible, however, also creates significant vulnerabilities in the system and the network because not all devices can be equipped with the necessary hardware and software to implement cutting edge security measures. This also gives attackers new ways to exploit vulnerabilities, requiring cybersecurity measures to be updated frequently. For example, ransomware attacks have become extremely common, where the attackers target institutions from a variety of industries, including government, education, healthcare, retail, finance, etc. Reports show that the number of ransomware attacks in 2021 is consistently higher than 2020, with damages expected to hit $6 trillion this year (up from $3 trillion in 2015). The most recent attack targeted Kaseya in July 2021, an IT management company. The attack is estimated to affect between 800 and 1500 small businesses, potentially making it the largest ransomware attack.

Since cybersecurity has become a critical issue, research, training, and job opportunities are increasing. For example, recently, it is reported that the Biden administration will prioritize cybersecurity in the distribution of $1 billion in federal IT funding. Similarly, it is reported that the US government is expected to spend more than $18B for cyber defense. This, in turn, leads to increased demand for cybersecurity experts. For example, the Bureau of Labor Statistics (BLS) projects a 32% job growth rate for information security analysts between 2018-2028. These jobs are expected to require higher education, including bachelor's and graduate degrees; and expertise in a variety of topics, including operating systems, networking, project management, and information systems. To meet this demand, colleges across the nation are building programs specifically targeting cybersecurity. Examples include the Information Security MS program in Carnegie Mellon University, Cybersecurity MS program in Georgia Institute of Technology, Advanced Cybersecurity program in Stanford University, to name a few.

Recently, Dr. Baris Aksanli and Dr. Duy Nguyen in the Department of Electrical and Computer Engineering received a grant from the Office of Naval Research to train the next generation of engineers who will be decision-makers with the skills to defend against emergent cyber and electronic warfare threats. The project aims to bridge the current gaps in cybersecurity training/research at undergraduate level by jointly addressing security of embedded systems, sensor networks, communication systems, and signal processing.

Dr. Baris Aksanli

Giving to the Electrical and Computer Engineering Department

To learn more about giving to the Electrical and Computer Engineering Department, please contact our Senior Director of Development:
Kate Carinder – kcarinder@sdsu.edu, or phone: 619-594-8264